

出國報告（出國類別：業務推廣）

「2019 以色列金融科技及
資安產業參訪」
出國報告

服務機關：中國輸出入銀行

姓名職稱：李培蘭 三等專員

出國地點：以色列

出國期間：108 年 05 月 25 日至 108 年 06 月 01 日

報告日期：108 年 8 月 7 日

公務出國報告提要

出國報告名稱：「2019 以色列金融科技及資安產業參訪」出國報告

頁數：20 頁

出國計畫主辦機關：中國輸出入銀行

出國人員：李培蘭 三等專員

出國類別：業務推廣

出國期間：108 年 05 月 25 日至 108 年 06 月 01 日

出國地區：以色列

報告日期：108 年 8 月 7 日

內容摘要：

以色列艱困的地緣政治環境及天然資源匱乏與台灣有相似之處，兩國在發展金融與銀行產業時也曾面臨各項挑戰，然而以色列政府透過金融創新改革政策，讓銀行體制更加健全，並加速國內金融科技的成長，躍升 FinTech 與資安強國，值得臺灣借鏡學習。

本次參訪活動是由中華民國銀行公會主辦「2019 以色列金融科技及資安產業參訪」，由金融聯合徵信中心郭建中董事長率團赴以色列，參訪「網路星光園區 (CyberSpark)」著名科技園區、政府單位、資安廠商、創投公司及相關數位金融特色銀行 Hapoalim Bank 及 Citibank 創新單位，透過面對面交流溝通，瞭解以色列資安、新創產業生態圈之現況及未來發展趨勢。

透過本次參訪活動，深入瞭解以色列在數位金融、資訊安全、金融監理與管理之發展，發覺以色列政府、軍方、學校、新創、創投等單位的互動機制及合作模式是其成為 FinTech 與資安強國之不可或缺重要關鍵因素，此行促成後續雙方在資安聯合防禦及新創產業合作交流的可能性。

目錄

壹、參訪目的	3
貳、參訪日期與行程	4
參、參訪過程與內容	6
肆、心得與建議	18
伍、附錄	19

壹、參訪目的

與台灣相距 8,000 公里的以色列，外交上孤立、沈重的國防負擔、天然資源貧乏，和台灣有許多相似的地方，兩國在發展金融與銀行產業時也曾面臨各項挑戰；然而，以色列政府透過經濟與金融創新改革政策，讓銀行體制更加健全，並加速國內金融科技的成長，同時也為新創環境打下一定基礎，而其完整的創新產業生態鏈成功模式，值得臺灣借鏡學習。

中華民國銀行公會與駐台北以色列經濟文化辦事處再次攜手合作，規劃「2019 以色列金融科技及資安產業參訪」，本次由金融聯合徵信中心郭建中董事長率團赴以色列，同行有金融監督管理委員會、中央銀行、財金資訊股份有限公司、金融研訓院及 7 家本國銀行等參與，共計 18 人，本次參訪「網路星光園區 (CyberSpark)」著名科技園區、政府單位、資安廠商、創投公司及相關數位金融特色銀行 Hapoalim Bank 及 Citibank 之創新單位，透過面對面交流溝通，瞭解以色列資安、新創產業生態圈之現況及未來發展趨勢。

透過本次參訪活動，我國銀行業可參考以色列對軟實力人才的培育和資安及新創產業發展模式，擴增國際視野，更可透過面對面交流討論，深入瞭解以色列在數位金融、區塊鏈技術、資訊安全、金融監理與風險管理之發展。期能藉學習以色列金融科技創新發展之成功經驗，作為我國金融產業相關規劃之指引參考，並促成後續交流合作。

貳、參訪日期與行程

活動日期	地點	時間	行程
5月25日			前往以色列
5月26日	特拉維夫 耶路撒冷		上午抵達以色列、進行半天文化參訪，下午返回酒店。
5月27日	特拉維夫	09:00-10:30	參訪：Checkpoint(資安公司)
		11:00-12:30	參訪：Radware(資安公司)
		15:00-16:30	參訪：CyberArk(資安公司)
		18:00-20:00	交流晚宴：以色列出口與國際合作協會(IEICI)邀請以方金融界、官方及業者參與交流
5月28日	特拉維夫	09:00-12:00	於以色列出口與國際合作協會(IEICI)聽取有關「Data & Infrastructure 數據和基礎設施」廠商簡報及交流
		14:30-15:30	參訪：Bank Hapoalim (以色列第一大銀行創新中心)
		16:00-17:00	參訪：Citi Lab (花旗創新實驗室)
5月29日	耶路撒冷	09:30-10:30	參訪：JVP 創投公司
		11:30-12:30	參訪：Ourcrowd 大眾募資平台
		14:30-16:30	參訪：Bank of Israel (以色列央行)
5月30日	貝爾謝巴	10:00-13:30	參訪：BaseCamp (新創公司孵化器) 參訪：Gav-Yam Negev 參訪：BGU Cyber Labs 參訪：CERT-IL 以色列網路管理局網路事故準備中心
5月31日-6月1日			返回台灣

參訪機構地址

1	Check point	5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel
2	Radware	22 Raoul Wallenberg street, Tel Aviv.
3	CyberArk	9 Hapsagot St., Park Ofer 2 P.O. Box 3143, Petach-Tikva
4	IEICI	29 Hamered St. 5th floor, Tel Aviv
5	Bank Hapoalim	Hapoalim, Menahem Begin 23, Tel Aviv
6	Citi Lab	Menahem Begin 121, 17th floor
7	JVP	Hebron Rd 28, Jerusalem
8	Ourcrowd	28 Derech Hebron, Jerusalem
9	Bank of Israel	Bank of Israel, P.O.B. 780
10	CyberSpark	Technologies Park, building #1, 4th floor

參訪行程簡圖



參、參訪過程與內容

一、 Check Point

CheckPoint 是全球首屈一指的資訊安全供應商，提供企業網路、資料與端點全方位的安全解決方案，擁有獨特專利技術，更是業界第一的防火牆領導先趨。

CheckPoint 介紹資安防護世代演進，從病毒、網路、應用程式至 Payload 分析防護，而迎接物聯網的時代，Gen V 更企圖以中央統一方式針對網路、端點、行動裝置、雲端進行完全控管防護。

綜觀目前網路威脅攻擊，橫跨國家及不同產業的方式進行大規模攻擊、利用政府投資之高價值科技、毀面性攻擊及多種面向攻擊（包含網路、端點、雲端及行動裝置），今後數位應用環境，不管是閘道、行動網路、終端裝置或雲端服務，皆可能成為駭客的入侵點及防禦破口處，透過其公司第五代防護管理系統 Infinity，提供完整的解決方案，其核心功能為「SandBlast Threat Emulation」及「SandBlast Threat Prevention and Extraction」，來偵測未知惡意程式、零時差攻擊及主動式預防資安威脅，在 Threat Extraction 技術，CheckPoint 針對檔案檢查推出「Clean Mode 及 Convert Mode」概念，可針對可疑郵件之附檔進行檔案重組及轉換，避免使用者點選惡意檔案進而觸發惡意執行程序及對外連線等作業。

二、 Radware

Radware 成立於 1996 年 5 月，公司總部設立於以色列特拉維夫，Radware 是全球領先的虛擬數據中心、雲端應用交付與網路安全解決方案供應商，其在 DDoS 防護（Distributed Denial-of-Service，分散式阻斷服務）或 Web 應用防火牆領域，有著獨特有效的偵測與防禦技術，穩居市場領導地位。

Radware 專家介紹銀行及保險業界面臨 DDoS 攻擊的趨勢與案例，

針對現在越來越普及的雲端服務應如何防護 DDoS 攻擊，建議可從三個面向進行著手：(一)與機構本身業務流程結合、(二)確保於攻擊機構服務仍不中斷、(三)與機構本身資安系統進行整合。

並邀請「Israel Discount Bank」進行實際案例分享，該機構自身曾遭受到大規模 DDoS 攻擊，其防護設備如 Web 應用程式防火牆、防火牆、入侵預防系統及 DDoS 等均失效時，如何透過與 Radware 協同合作，順利度過危機。

Radware 的現任執行長也分享了自身經歷，他曾在以色列軍方服役超過 5 年，累積相當的技術、經驗與人脈後，與幾個志同道合的朋友共同創辦了這間公司，從最初員工不到 10 人，成長至今在全球 40 多個國家設有辦事處與分公司的規模。

三、CyberArk

CyberArk 1999 年成立於以色列，專注於特權帳號安全，是第一家 2014 年在美國 NASDAQ 上市的以色列資訊安全公司，特權帳號管理解決方案的領導者，於 2018 年 Gartner Security and Risk Management Summit 獲選為 Top 10，排名第一名之安全專案「特權帳號管理 (Privileged Account Management)」。

CyberArk 與我們技術分享，介紹駭客入侵攻擊手法，說明駭客最終攻擊目標都是機構重要營運系統，獲得特權帳號以竊取資料或影響其服務效能，妥善管理特權帳號可以破壞駭客攻擊鏈，駭客會針對「特權帳號」進行入侵，主要有下列步驟：

- (一)尋找需提權才能存取的資產，通常為機構內部重要資產或機敏資料，如個資或金融機敏資訊。
- (二)進行提權，通常利用帳密竊取工具竊取高權限帳號，或是利用系統漏洞進行提權作業。

(三)進行橫向移動並執行內部網路偵查作業，尋找機構內部重要營運系統。

特權帳號為企業現今所面臨的最大資安漏洞之一，幾乎外界攻擊都會利用這些高權限的帳號，來取得控制組織的資源以及存取大量機敏資料，對特權帳號管理、連線監控及保護是有其必要性。

四、 以色列出口與國際合作協會 (The Israel Export & International Cooperation Institute)

以色列出口與國際合作協會(以下稱 IEICI)是一家非營利組織，功能與臺灣的外貿協會相仿，由以色列政府和私有部門提供支持，做為以色列企業對國際市場聯繫平台，旨在促進海外企業和以色列公司建立業務關係、組建合資企業以及結成戰略聯盟，並透過會展、考察團等各式活動，協助以色列國內企業將產品與服務帶向國際市場。

IEICI 致力於讓潛在客戶與能滿足需求的以色列相關製造商相互聯繫，確保全球各地企業亦能從以色列頂尖科技產業的創新與品質中獲益。

在參訪行程中，首先介紹以色列如何藉由產、軍、學三角來發展整個 Fintech 生態，布局在付款(Payment)、借款與財務(Lending & Financing)、區塊鏈與虛擬貨幣(Block Chain & Virtual Currencies)、財富管理與資本市場(Wealth Management & Capital Market)、保險業科技(INSURtech)、監管科技(REGtech)…各種領域，並使用人工智慧、大數據以及分析(AI, Big Data & Analytics)等技術來進行創新突破與協同作業，在蓬勃發展之下產生了很多的成功案例，值得我們在策略面效法、跟進。

接著是由資安管理專家 Dr. Amir Schreiber 說明金融界遭受資安攻擊的嚴重性，每年經由 ATM 或是跨行交易的損失高達 10 億美元，而攻擊的事件正在逐年增加。

接著也說明了這種組織型犯罪的共犯結構，是由首腦、錢駱集團、電腦病毒作者、惡意軟件及其散播者、散漫的系統管理者、不嚴謹的金融機構經理人等有意或無意所構成。

要降低金融資安風險，需要從提升資安技術與加強管理流程雙管齊下，而且必須不斷的思考，無論是從已知的已知、已知的未知，進而探索未知的未知，多一層防範，就多一層助益。

五、簡報廠商「Data & infrastructure 數據和基礎設施」

(一)DBH-S

是一家總部位於耶路撒冷的技術公司，提供異質資料庫即時訊息整合解決方案，其下產品 CR8 整合企業內部異質資料庫，不管是 SQL 和 NoSQL 數據庫，以即時方式將關鍵系統日誌以連續流方式傳輸到目的數據庫，從而提供即時高價值、高核心的內部營運和業務數據分析，所利用的技術不會對來源系統造成執行效能負擔，且可以匯集到其他系統再利用。

目前在美國前五大銀行都有使用其產品，從 50 多個重點系統，整合異質資料庫產生即時資訊，以提供客戶導向之大量數據分析來源及機器學習預測的基礎。除銀行業、保險業、全球電力能源公司、汽車製造業、遊戲公司等都有導入，提供各方面預測分析再利用。

(二)OpenLegacy

是一家年輕的新創公司，是以微服務 (Microservices) 為基礎架構，提供自動化應用程式介面 (Application Programming Interface, 簡稱 API) 創建、優化、測試、部署和管理，涵蓋整個 API 生命週期。專利方法繞過複雜的層次，擴展核心系統業務邏輯，提供 Web、行動裝置或雲端使用，以 Java、RestAPI 或 SOAP

等形式提供。最重要的是，其縮短了 API 開發週期並節省了大量成本，這個過程不僅快速、簡單而且安全，也不需要特殊的人員技能或對現有系統、架構進行變更。

(三)Centerity

是智慧維運管理解決方案 (Artificial Intelligence for IT Operations)，提供企業級資安監控和性能分析平台，可提高持續運營系統的可靠性，以確保關鍵系統的可用性。此方式大幅降低維運人員的管理負擔，透過監控各項設備訊息，包括應用程式、大數據、操作系統、數據庫、存儲、計算、安全、網絡、雲端和 IoT 設備，評估來自整個訊息及參考內部運營技術指標，進行性能分析，提供整合式動態業務服務視圖瀏覽、各項效能顯示及問題預警，以提早識別系統問題癥結。

(四)Privacy Rating

是一家監管技術的初創公司，其產品 qprivacy 解決方案適用於所有平台，防止從用戶端在瀏覽公司網站或使用其應用程序時，收集未經授權的私人訊息，可以處理所有類型通信，包括加密或非結構化數據，進而保護用戶端個人隱私資訊，而不影響原系統性能及用戶體驗。

六、 以色列工人銀行 (Bank Hapoalim)

以色列工人銀行目前是以色列第一大商業銀行，其總部位於特拉維夫，在以色列全國共有 280 多家分行，與科技業巨頭微軟合作，開發區塊鏈的數位銀行擔保 (bank guarantee) 平台，利用此平台，客戶無須親自到銀行辦理業務，而是在極短的流程中透過數位化、自動化和安全的方式接收擔保文件，此區塊鏈技術使用可大幅提升顧客體

驗，以及增進顧客對銀行系統信任程度。

本此參訪是工人銀行金融科技創新中心，在其總部設有一整層辦公區間，其設計風格採活潑無間隔的通透環境設計，與一般辦公室設計迥異，處處獨俱巧思，參觀那天正值公司舉辦員工慶生活動熱鬧愉快。其職場的文化較無階級意識，對事情的態度相當直接，可以接受各種不同的想法，當提出反對意見或不同的解決方法時，不但不會被「另眼看待」，反而是被鼓勵的。該中心負責人認為團隊合作首重溝通，專案成員需充分討論與密切合作，鼓勵同仁暢所欲言，隨時可在專案進行中提出質疑與想法，一旦採納隨即調整，因此各種創新的想法源源不絕，該中心負責人並強調創新態度，心態上一定不能怕失敗，必須勇於探索，不斷嘗試，雖該單位近 3 年創新實驗成功率僅有 5%，卻仍獲管理高層支持。目前國內台灣銀行也於今年規劃成立創新實驗室（InnoLab）。

七、花旗創新實驗室（Citi Innovation Lab TLV）

花旗創新實驗室成立於 2012 年，係花旗銀行(Citi Bank)旗下的一個國際性金融科技創新基地，花旗推動 FinTech 創新的單位主要是加速器(Accelerator)和創投(Venture)。

加速器是花旗與新創企業合作的橋樑，導入組織外部創新能量的重要渠道，為深化雙方的互惠合作，花旗提供給新創企業的支援包括：創業輔導、市場網路連結與開發、IT 系統等。對於潛力優秀的新創企業可獲得花旗創投(Citi Venture)的資金挹注，新創企業藉由和花旗合作獲得資源，花旗則藉由參股分享新創企業之成長果實，雙方互蒙其利。

(一)花旗加速器(Citi Accelerator)成就

- 有 80 家公司從 8 類計畫中成功出場
- 從花旗加速器成功出場之公司資金募集達 7.5 億美金
- 有 5 家被其他企業併購

(二)以色列歷年金融新創公司的數量（在以色列首都特拉維夫每 290 個人就有一個從事新創）

年份	2012	2013	2014	2015	2016	2017
數量	159	210	283	253	419	475

八、JVP 創投公司（Jerusalem Venture Partners）

JVP 是一家成立於 1993 年的風險投資基金公司，總部位於耶路撒冷，以色列最大、也是全球前十大創投基金，勇於扶植當地資安新創，目前管理的投資金額高達到 1.4 億美元，投資企業超過 130 家，並有 12 家在納斯達克上市，其中最著名的案例是 CyberArk 孵化項目，目前 CyberArk 已是全球知名的網絡安全公司，在美市值高達 20 億美元的上市成功公司，而 2015 年阿里巴巴集團也成為 JVP 7 期基金的戰略投資人。

JVP 介紹近 20 多年來投資主要關注的領域，從通訊、企業級儲存及軟體、網路安全及人工智慧應用到破壞性創新（Disrupt Markets Through Technology），未來破壞式技術（disruptive technology）如資安、人工智慧、機器深度學習、大數據、雲端、儲存、行動裝置及物聯網等技術，在各方面領域都會充滿商機。

以色列高科技業除靠政府計畫性扶植外，創投業也是最重要推手之一，JVP 選擇初創公司十分嚴格，一旦選擇就會開始重度孵化，JVP 的孵化器平均時程是 18 個月，JVP 會在研發、銷售、人力、資本等各方面給予創業公司支持和指導，在整個孵化的過程，JVP 扮演著非常重要的角色，除了協助外 JVP 也會選擇投資，同時深度參與公司成長，積極提供各類資源，然而所有投資不可能皆獲成功，JVP 對於增長無望項目，一旦發現失敗，就立即清算。

九、OurCrowd 大眾募資平台

OurCrowd 創立於 2013 年，是位於耶路撒冷的大眾籌資平台，被「賀芬頓郵報」稱為「目前全球最成功的股權群眾募資平台」，專注於新創產業，首要任務是確保投資人與籌資公司皆能在其平台上互謀其利，創造雙贏局面。

OurCrowd 嚴格審查籌資公司，平台篩選錄取率不到 2%，以確保公司是具有前景且有獲利潛力，對投資人資格也設有條件，以確保擁有較高風險承擔能力，只有年收入在 20 萬美元以上或者是淨資產達 100 萬美元以上才能加入成為 OurCrowd 會員。

與台灣股權募資平台最大的不同在於以色列允許平台經營業者認購籌資公司的股份，OurCrowdy 亦設有基金專門投資其平台上的籌資公司。

十、以色列央行 (Bank of Israel)

以色列銀行成立於 1954 年 12 月 1 日，為以色列的中央銀行，位於耶路撒冷，獨立於政府行使職能，主要負責制定和實施貨幣政策、管理外匯儲備、監督以色列各類銀行、發行貨幣。該行代表與我們分享了以下的經驗：

(一)以色列銀行體系

1. 五大主要銀行機構的整體表現：包含 4,500 億美金的資金往來活動、8~9%的股東權益報酬率、42,000 員工等概觀數據等經營指標。
2. 財務體系近期的變化：包含非銀行機構的金融實體(如：信用合作社、P2P、非銀行信貸提供者、機構投資者)以及因應法規遵循所產生新的競爭者(如：協助處理電腦化問題、新科技的發展)加入市場，以上所提兩股力量的挹注，推升了以色列金融的整體

競爭力。其目的是建立一種金融機構共同合作的環境，以促進更多的市場參與者加入。

3. 主要的挑戰與風險

- 業務模式的變化
- 網路、資安、資料保全與個資的維運風險
- 未來財務體系的新競爭
- 在進行跨國或業務執行以及逃漏稅所產生違規風險
- 房地產市場相關抵押貸款的風險揭露

4. 銀行體系前五大困擾的議題為：網路安全、法規遵循、科技及永續經營、顧客、櫃台實務。

(二)新創與科技的規劃架構

1. 成立科技與創新部門，其主要功能與職責：法規遵循與執行、金融科技的創新、網路監管。
2. 調整網路銀行的法規：允許完全的電子銀行的存在、移除網路銀行交易活動的阻礙。
3. 執行的業務：駐點檢查、規範銀行之科技風險評估、提升網路銀行系統的資安完備度、隨時更新法規、衡量並分析使用者包含數位化的直接交易方式。

(三)網路風險管理

1. 資料外洩的狀況：2018 年全球有 41,686 網路攻擊發生在 180 個國家，已確認資料外洩達 2,013 次，其中 71%是與財務、經濟相關，而這些外洩事件 56%都是事隔超過一個月才被發現。
2. 網路風險與資訊風險的差異：範疇不同、對手不盡相同、攻擊性質不同、造成的影響不同。
3. 因應網路攻擊的方式應該是網路防禦，而非網路安全。網路風險可分為：資料外洩與盜取、金錢盜取、功能中斷或服務拒絕、資料毀損。

4. 網路防禦的管理重點

- 複雜且背後有資金挹注的網路攻擊是無可避免的
- 網路攻擊不只是網路專業人員的問題
- 需有不同層次的防禦
- 不能光以技術來衡量
- 網路防禦需具備主動性、前瞻性、創造性
- 需不斷檢視各個執行面上控管點之有效性

5. 對法規的期許

- 以原則性取代規則性－重點在於該做什麼，而不是該怎麼做
- 參照國際標準
- 與其他的法令相容
- 需定期的檢視、更新

十一、 BaseCamp 新創公司孵化器

BaseCamp 是以色列相當具有特色的新創公司孵化器，位於 Gav-Yam Negev Advanced Technologies Park 高科技園區，致力於發掘具有潛力的學術研究團隊，並協助該團隊創業，挹注創業過程所需的資源和專業，讓這些團隊能順利募得資金，進而讓研究成果走向市場。

BaseCamp 表示經濟發展是將自然資源推進市場，然而 21 世紀的經濟發展是利用創新與科技，創造高品質的工作機會。

對於新創的發展提供了以下的管理服務：觀念(Concept)、政府支援(Government Support)、設計(Design)、社群(Community)、學術(Academy)、高科技公司(High-tech Companies)。而資源來自於三個方面：公司間的結伴、學術界的催化、政府的支援。

在未來與臺灣合作契機方面：臺灣高科技領域的人才與技術資源相當充沛，會是他們獲取創新科技的重要來源，與他們能達到互補效果。今年 2 月與中山大學簽署合作備忘錄，雙方互設辦事處作為連結在地的加速器，並交換研究與企業產學合作，為兩方在新創投資、併購和科技研發上有更多合作的可能性，並積極尋求商機創造價值。

十二、 Gav-Yam Negev

成立於 2016 年，致力於新興科技的發展，透過產官學三方緊密合作孕育出的產業生態圈，提供人才與創新科技發展平台，期能與政府、產業及投資者共創三贏。目前由以色列政府、貝爾謝巴市、Ben-Gurion 大學、KUD 國際管理顧問公司、Gav-Yam 資產與建築機構以及國際科技大廠(如：IBM、甲骨文、DELL 等)所合作打造，提供了策略發展、經營管理、辦公環境、產業關係、政府行政等多面向的整合性服務。

園區的發展狀況：目前已有 2,500 位工程師進駐在園區內 70 家公司，其中 86% 是當地居民。建築物部分已完成 3 棟，2 棟在建中，還有一棟已完成設計規劃，目前園區未來發展規劃如下：

目標年份	2019	2024	2029
進駐人數	2,500	4,000~5,000	10,000+
辦公大樓數量	3	6	15

十三、 CERT-IL 以色列網路管理局網路事故準備中心

成立於 2014 年，由以色列政府為強化網路資安防護設立之官方機構，為以色列網路管理局 (Israel National Cyber Directorate，簡稱 INCD) 轄下網路事故準備中心 (Cyber Event Readiness Team，簡稱 CERT-IL) 設置於 Gav-Yam Negev 園區，其主要之任務是當以色列機構或是民間單位發生資安事件時，由各領域專家提供相關之諮詢以協助資安事件應變處置，其設立 Computer Emergency Response Center 提供 7*24 熱線服務，機構或民眾如遇資安事件可透過電話或電子郵件得到必要協助。

CERT-IL 提供資安事件通報與資安資訊分享平台，讓其下會員資訊分享及經驗交流，會員不會因揭露資訊而承擔法律責任，其平台定時發布資安相關訊息，並提升民眾對訊息安全及隱私課題的認識，該

機構也成立國家級的資安監控中心(Security Operation Center, SOC)以掌握國家整體資安威脅態勢，同時也與國際各國進行合作，以達國際資安聯防之效。

本次參訪成員有本國金融資安資訊分享與分析中心同仁，會中進行經驗交流，達成兩機構未來合作共識，是為此行最大收穫之一。

十四、BGU Cyber Labs

本古里安資安實驗室(BGU Cyber Labs)是 Ben Gurion 大學的一個傘式組織，是一個很活躍的學術單位，申請很多專利，研究方向為各種網絡安全，大數據分析和 AI 應用研究。

園區裡的本古里安大學(Ben-Gurion University, BGU)扮演關鍵的靈魂角色，本古里安大學成立於 1969 年，是以以色列首任總理名字命名，儘管建校時間不長，卻已躋身全球頂尖科技大學之列，成為培養網路安全人才的搖籃。目前在校學生約有 20,000 人，其中一半以上攻讀電腦科學、工程和自然科學。

此次參訪，此單位介紹一些研究並做展示：

Game of Drones of Drones - Detecting Captured Target from an Encrypted Video Stream 研究，展示該技術偵測非法無人機視頻拍攝，該研究解決人們越來越關注無人機用於個人和商業應用影響隱私之議題。

Injecting and Rremoving Lung Cancer from CT scans 研究，展示攻擊者如何在醫療機構中植入惡意設備的視頻，並修改 3D 醫療掃描，並以添加或刪除嚴重疾病的證據，如癌症，目前醫院很多設備暴露在互聯網上，醫學圖像數據許多透過網絡傳輸而不加密，很容易遭受中間人攻擊和操縱。

肆、心得與建議

以色列地處中東火藥庫，以一個國土面積約台灣 60%，人口約台灣 36%的國家，且國土絕大部份都是沙漠，天然資源十分缺乏，卻成為全球聞名的資安、新創之國，甚至朝著全球人工智慧產業中心發展。而這麼斐然的成就背後不乏政府有遠見的規劃、學術界人才積極培養與民間企業努力發展的影子。

在這次訪問後，整理了這些資料，發覺他們的布局相當周密完整，從增加國際交流、促進商機的色列出口與國際合作協會（IEICI），推動與培植新創產業的以色列創新局、科技產業園區與孵化器，推動與規劃整體 FinTech 制度的以色列央行(Bank of Israel)，培育新創、FinTech 以及資安人才的大學教育制度，而在民間，更是不乏資金募集平台、創投公司、銀行的創新實驗室、以及眾多的資安科技公司，並建有互動機制及合作模式，其完整創新產業生態鏈成功模式，值得我國借鏡學習。

我政府近年除積極推動「五加二產業創新計畫」外，另提出「優化新創事業投資環境行動方案」，以五大主軸：(一) 充裕新創早期資金、(二) 人才發展及法規調適、(三) 政府成為新創好夥伴、(四) 提供新創成功出場管道、(五) 新創進軍國際市場，以加速人工智慧、物聯網、金融科技、無人載具等產業發展，期望能多加取法以色列，以官、學、產多管齊下的方式，讓台灣急起直追，位列全世界新創以及 FinTech 高度發展的國家之中。

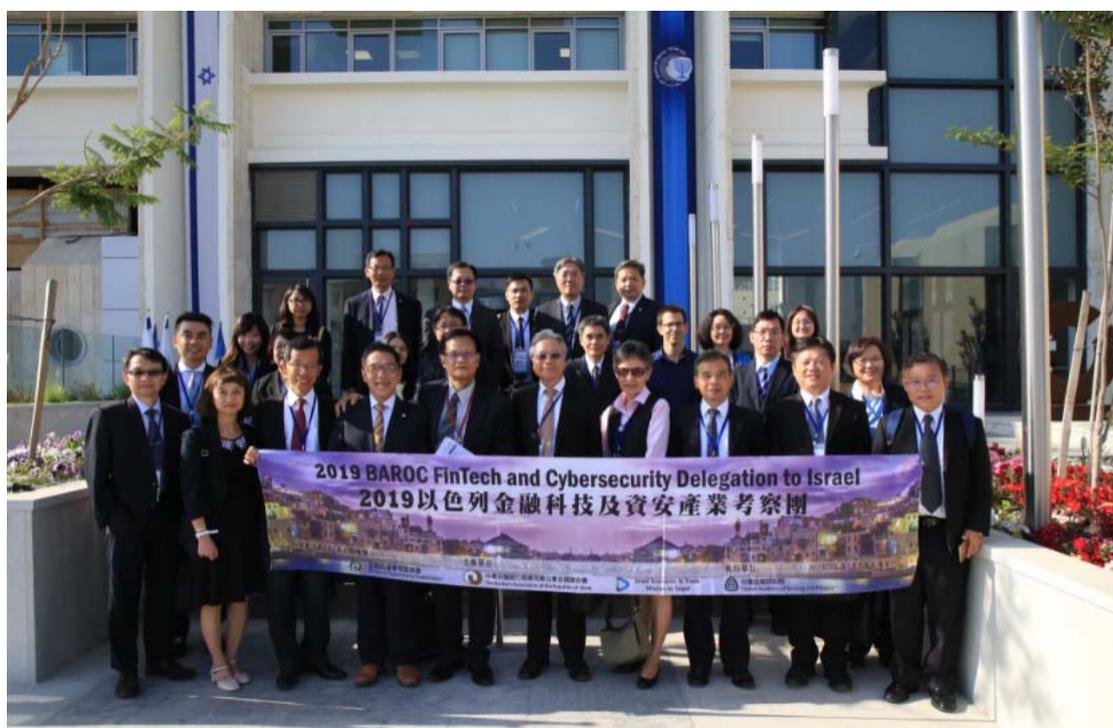
近年來資安議題在國內快速升溫，從引發全球恐慌的 WannaCry 及 Petya 勒索軟體，到遠東銀行遭駭客入侵、台積電受病毒感染事件以及近期銓敘部發生 59 萬筆文官個資外洩，顯示資安防護的重要性，要降低金融資安風險，需要從提升資安技術與加強管理流程雙管齊下，除了藉用各項資安設備加強對外防護監控，更重要提升內部人員資安防護意識。

伍、附錄

參訪團員

項次		姓名	機構名稱	職稱
1	團長	郭建中	金融聯合徵信中心	董事長
2	副團長	雷仲達	合作金庫商業銀行	董事長
3	團員	蔡福隆	金融監督管理委員會/資訊服務處	處長
4	團員	廖英傑	金融監督管理委員會/銀行局	副組長
5	團員	李瑞杺	中央銀行/資訊處	副處長
6	團員	黃崇哲	台灣金融研訓院	院長
7	團員	郭春明	合作金庫商業銀行/董事會秘書部	主任秘書
8	團員	王堯德	國泰世華商業銀行/資訊安全部	協理
9	團員	方振維	財金資訊股份有限公司/安控部	協理
10	團員	陳嘉宏	財金資訊股份有限公司/安控部	組長
11	團員	蘇清偉	富邦金控	副總經理
12	團員	王靖欽	富邦金控/資訊處	資深協理
13	團員	劉美玲	玉山銀行/信用卡暨支付金融事業處	副總經理
14	團員	邱顯堂	臺灣銀行/資通安全處	處長
15	團員	張銘志	臺灣銀行/電金部	副經理
16	團員	李嘉銘	玉山商業銀行/數位金融事業處資訊發展部	技術協理

項次		姓名	機構名稱	職稱
17	團員	周芷維	玉山商業銀行/數位金融事業處	代襄理
18	團員	李培蘭	中國輸出入銀行/資訊安全管理中心	專員
19	工作人員	楊 柑	中華民國銀行公會	秘書長
20	工作人員	溫國恩	中華民國銀行公會業務組	組長
21	工作人員	張美華	中華民國銀行公會業務組	專員
22	工作人員	曹慧蘭	中華民國銀行公會業務組	助理幹事
23	工作人員	鄭凱名	中華民國銀行公會業務組	助理幹事
24	工作人員	張凱君	台灣金融研訓院金融訓練發展中心	副所長
25	工作人員	林秉貞	台灣金融研訓院海外業務發展中心	專案副理



參訪團員合影